View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Institute of Advanced Engineering and Science

International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 4, August 2020, pp. 4168~4175
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i4.pp4168-4175

Internet service providers responsibilities in botnet mitigation: a Nigerian perspective

Olatunji Okesola[1], Marion Adebiyi[2], Tochukwu Osi-Okeke[3], Adeyinka Adewale[4], Ayodele Adebiyi[5]
[1]Computational Sciences Department, First Technical University, Nigeria
[2,5]Department of Computer Science, Landmark University, Nigeria
[2,5]Department of Computer and Information Sciences, Covenant University, Nigeria
[3]Department of Mathematics and Computer Sciences, Afe Babalola University, Nigeria
[4]Department of Electrical and Information Engineering, Covenant University, Nigeria

Article Info

Article history:

Received May 30, 2019
Revised Feb 3, 2020
Accepted Feb 24, 2020

Keywords:

Botmaster
Botnet
Incentives
Internet service provider
Mitigation
Nigeria

Corresponding Author:

Marion Adebiyi,
Department of Computer Sciences,
Landmark University,
Omuaran, Kwara State, Nigeria.
Email: ayo.adebiyi@lmu.edu.ng

ABSTRACT

Botnet-based attack is dangerous and extremely difficult to overcome as all the primary mitigation methods are passive and limited in focus. A combine efforts of internet service providers (ISPs) are better guides since they can monitor the traffic that traverse through their networks. However, ISPs are not legally banded to this role and may not view security as a primary concern. Towards understudying the involvement of ISPs in Botnet mitigation in Nigeria, this study elicited and summarized mitigation measures from scientific literatures to create a reference model which was validated by structured interview. Although, ISPs role is seen to be voluntary and poorly incentivized, the providers still take customers security very serious but concentrate more on the preventive and notification measures.

Copyright © 2020 Institute of Advanced Engineering and Science.
All rights reserved.

1. INTRODUCTION

A network of infected computers or machines is called a Botnet and each of these computers is referred to as a Bot. Hence, a botnet is a connection of compromised computers controlled by a Botmaster who distributes attacks over hundreds of computers across the Internet [1]. The cumulative bandwidth and large number of attacks make botnet-based attacks dangerous and difficult to overcome. In 2009 for instance, BredoLab created an estimated thirty million bots, the 'Star Wars' twitter botnet. Though its purpose is still unknown, the botnet is said to have compromised over 350,000 twitter accounts [2]. One of the popular and largest botnets attack was Citadel [3] where keyloggers were installed onto victim's computers thereby enabling botmaster to monitor keystrokes on the infected systems. Over five million keystrokes of users across the globe were logged resulting to over five hundred million dollars loss [1, 3].

Unlike other Internet malware, the control communication network of a botnet is its unique feature. As illustrated in Figure 1 with the arrows showing the direction of network connections, bots in the botnet connect to special hosts - command-and-control (C&C) servers, who forward commands from botmaster to the other bots in the network for a possible attack.

Nigeria is a country with a very high internet coverage with quality wired and wireless connections. Unfortunately, she is a key player in cybercrime and has become an ideal target for botnets being a major source of Spam [4, 5]. This may be linked to the fast growth of Internet usage owing to the explosion of internet service providers (ISPs) - organisations that provide Internet services as well as software packages and e-mail accounts [6].

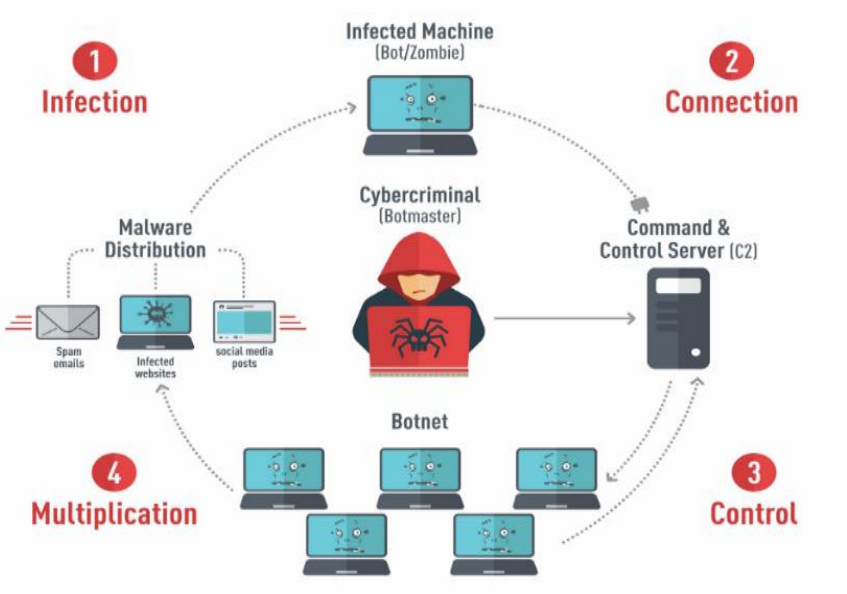

Figure 1. How a botnet work [7]

Prior to 2013, four primary methods commonly being used to mitigate DDoS attacks were commercial security software, criminal enforcement, botnet seizure by federal agencies, and private civil action [8]. However, such efforts, though valuable, are passive and limited by their focus on prevention [9, 10]. A leading cloud based service provider, CloudFlare, therefore offered DDoS protection capable of matching sophisticated DDoS attacks. This was more effective but Sood et al., [3] and Lone et al., [8] argued that improved result is possible with boundless and collaborative efforts of both the private and public organizations in Nigeria including the ISPs, economic and financial crimes commission (EFCC) and Cybercrime Prevention Working Group. This study therefore aims at investigating the role of ISPs in Nigeria towards ascertaining their capability of combating botnets in isolation. Following a review of related studies in the next section, an overview of incentives that attract ISPs to botnet mitigation is provided along with a reference model, while a table of mitigation measures for ISP are summarized in the later part of this study.

2. RELATED WORK

Modular Integrated Services Limited [11] highlighted a bigger picture of numerous recommendations developed by International Telecommunication Union to secure telecommunications infrastructure and associated services or applications where implementation of the international information society management standard was presented as the most comprehensive approach to combat botnet. Nonetheless, quantitative analysis [7, 8] have always presenting ISPs as the better guide against botnets due to their functional indispensable responsibilities. Nabil [12] therefore gave a classification that reflects the lifecycle and current resilience techniques of botnets by analysing commonalities from a network providers' perspective to design and implement mitigation strategies against botnets.

ISPs view customers-security role as voluntary since they have no legal binding to secure their customers [6] but they are in an optimal position to provide security to internet users [9]. Meanwhile, Empirical study and literature review of Timo et al. [5] claimed that no organisation can effectively combat botnets in isolation but in conjunction with one and other. However, Van Eeten et al. [13], recognised ISPs as a key control point, in their study of spam traffic where data were collected on the location of infected machines over time to examine the role of ISPs in mitigating botnets. This validates Stamatoudi's functional definition of an ISP as "a passive carrier that must block material access upon receiving notice of an alleged malware" [14].

Noting that ISPs in Nigeria may be unaware of the vulnerabilities the use of their infrastructure is posing, Longe et al., [1] conducted a survey on the impact of ISPs against botnet. Leaving chi-square at 0.05 level of significance, their descriptive statistics showed that the level of security provided against crime by ISPs are relatively low resulting in a positive relationship between the level of internet crime and the attitudes of ISPs to their networks safety. Hence, Brent et al., [9] believed that ISPs should be motivated and therefore proposed a further study to identify how best ISPs could be incentivised.

3. RESEARCH METHOD

A literature survey and empirical study were conducted to examine mitigation measures (Nigerian) ISPs have taken, those they could have taken, and others they plan to take against botnet. This specific was to identify botnets C&C-structures and their relevant features. A 'reference model' summarising mitigation measures such as technical, organisational and juridical measures was used. The empirical study was restricted to Nigeria as interviews were conducted to validate results obtained from the literature study. The interviewees are security officers and service managers at top Nigerian ISPs who have a clear understanding of the incentives and mitigation measures.

4. ISPs AND SECURITY INCENTIVES

Since ISPs know what traffic traverses their network, they are in the best position to detect malicious traffics and quarantine the infected computers in their network [4]. Hence, they are mostly expected to take the responsibility of mitigating spam, computer viruses, fraudulent email, and spyware [15] However, since they are not the root cause of attacks and mitigation comes with its own cost, ISPs may be unwilling to take action if the responsibility does not attract incentives/factors. Hence, Quantitative analysis [7, 8] attributes lack of incentives as a major factor responsible for a low action rate in botnet mitigation since. Since ISPs naturally respond to economic (customers support, price, etc.) and non-economic (peer pressure, peer recognition, etc.) incentives [16], incentives are those factors considered by both the individual and organizational decision-makers to mitigate botnets.

4.1. Organisational incentives

These are factors that ISPs have some levels of controls over which may include business model. priority given to security, cyber-insurance, awareness and training, participation in security efforts, size of customer base, cost of customer support, cost of management abuse, and cost of infrastructure expansion [17]. The bigger ISPs generally perform better but they experience high security attacks and possibly high invention [16], thereby invest more in cyber-insurance. Similarly, the higher the usage of pirated software, the higher the ISP's exposure to botnet, and the higher the security awareness of customers and staff, the higher the competences and the lower the level of botnet attacks.

Since "Very large ISPs are effectively exempted from peer pressure as others cannot afford to cut them off, much of the world bad traffic comes from the networks of these too big to block" providers" [14]. However, large ISPs has lower infection rates than small ISPs [17] because they are highly automated to identify, notify and mitigate infected customers thereby making the mitigation process economically efficient [4].

4.2. Institutional incentives

These are factors beyond ISPs' direct control but instituted by the policy makers or market conditions. They are defined legal frameworks in which ISPs operate and include cyber-security laws and regulations, blacklisting, peer pressure, reputation effects, competitive cost pressure, cost of customer acquisition, and cost of technology mitigation [17]. Regulation - an effective incentive [18] - requires cyber security incidents be nationally mitigated [19] since national anti-botnet centre usually are hardly infected. National initiatives on botnet mitigation should therefore be promoted and good models circulated [20] while policy makers give ISPs more incentives for taking action [2]. Hence, ISPs are being pushed by regulatory bodies such as internet engineering task force (IETF) and Organisation for Economic Cooperation and Development (OECD) to clean-up their customers infected computers [21].

Where ISPs are mostly driven by institutional incentives, they are expected to perform same in terms of botnet mitigation as incentive structure may have to be changed if they are to increase their efforts [16]. However, since ISPs perform very differently when exposed to both comparable institutional incentives and economic circumstances [16], the country-level mitigation measures cannot be sufficient unless organizational incentives are addressed and realigned together.

4.3. Organisational vs institutional incentives

The incentive structure of an ISP is a function of the institutional and organizational factors – the sets that are closely interrelated and very difficult to separate. While policy makers postulate institutional incentives, organizational ones are being determined by the individual ISPs in line with the institutional incentives. Much [18, 22] have been done on the incentives of ISPs to improve security, and some have been identified as enhancing security while others work against it. However, the net effects of these incentives on each ISP is still unclear as the ISPs behave differently when exposed to similar incentives. It is therefore important to know how much discretion each ISP has for botnet mitigation. Every

ISP should decide how to mitigate botnet and determine their organisational incentives even when faced with a common set of institutional incentives as defined by the country legal framework [16]. ISPs' attitude towards botnet mitigation is mostly determined by institutional incentives. However, their varying behaviour when subjected to same incentives suggests that legal framework on its own cannot be sufficient to mitigate botnet unless organisational incentives are also addressed and properly aligned [8].

4.4. Best practices and incentives

Although, most Nigerian organisations are ill-equipped to mitigate malware threats, studies have shown that organisations cannot effectively mitigate botnet in isolation [5]. Both private and public organisations collaborate to fight botnet but the individuals and corporate entities in the private sector still remains the biggest victim of cybercrime [23-25]. Towards fighting against all forms of financial and cyber-crimes therefore EFCC was setup and empowered by Nigerian government to work hand in hand with the cybercrime Prevention Working Group to combat financial crimes.

Internationally, organizations such as anti-phishing working group (APWG), communications security, reliability and interoperability (CSRIC), European network and information security agency (ENISA), IT Association for telecommunications, messaging, malware, and mobile anti-abuse working group (M3AAWG), and online trust alliance (OTA) have come together for the sole purpose of mitigating botnet. Different initiatives such as internet exchange point of Nigeria (IXPN) and Association of Telecommunications Companies of Nigeria are empowering stakeholders on capacity building and encouraging synergy amongst the various agencies. This is because training, awareness, and public empowerment on cyber security services, strategy, and intelligent building should go ahead of cyber criminals [1, 26], as public and private organisations have to reconsider their approaches to cyber threats in order to establish the required security practices on the critical IT infrastructure [23]. ISPs should therefore consider, as a top practice, awareness and training, continuous monitoring and log analysis, vulnerability and patch management, continuous risk assessment and treatment, management services and independent reviews [23]. Nigeria as a country, also has to continuously invest in research, build local cyber threat management infrastructure to improve her ability to anticipate, detect, respond and contain cyber threats.

5. THE REFERENCE MODEL

This section presents a reference model (Table 1) similar to [4] where botnet mitigation measures for ISP are summarised. The model is in line with structure of anti-botnet lifecycle and ecosystem defined by the online trust alliance - OTA [20]. The sequence of the five stages - prevention, detection, notification, remediation and recovery - makes up an anti-botnet lifecycle presented in Figure 2 where:

- Prevention - proactive measures of an ISP to avert user's devices from potential attacks.
- Detection - measures to identify threats, vulnerabilities or attacks on the ISP's network.
- Notification: measures taken by ISP to alert customers of security breaches.
- Remediation: corrective measures initiated by an ISP to clean compromised system of malicious software.
- Recovery: activities of an ISP targeted at regaining the impact of an attack.

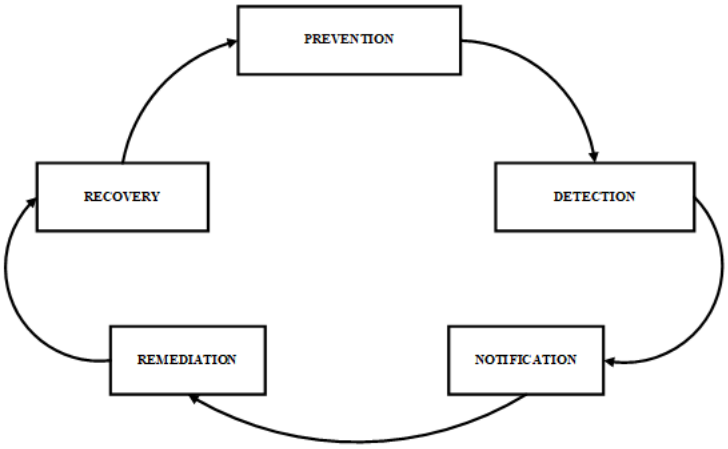

Figure 2. Anti-botnet lifecycle [4]

5.1. Mitigation measures

Telecommunications Act [27] mandates ISPs to protect their customers against cybercrime following Technical, organizational and legal measures as postulated by Asghari [28]. Similarly, ISPs are expected to tell their customers the risks related to the use of web services they offered by the ISPs, as well as what customers ought to do to scale down these risks. However, the Act [27] is silent on the role of ISPs when botnet is detected in its network thereby implying that ISPs action against botnet is not obligated by law. Having elaborated on the general botnet mitigation measures, this study adapted those measures derived by [4] to determine whether each measure observed by ISPs is aimed at their customers, the ISP itself or other stakeholders. The study is also aiming at knowing whether the measure is technical, organizational, or legal. The research findings are as presented on Table 1 following a detailed explanation of the lifecycle stage.

Table 1. The reference model

Target set	Aspect	Description	Technical	Organizational	Legal
PREVENTION					
Customer	PC-1	Customers are provided with endpoint security solutions	o	o	
	PC-2	Customers are always educated on botnet threats and mitigation	o	o	o
Other	PO-3	ISPs share information on botnet mitigation through collaboration		o	
	PO-4	There is collaborative initiatives for botnet mitigation		o	
ISP	PI-5	Intrusion prevention system (IPS) is being applied	o		
	PI-6	Technical measures are applied against botnet infections	o		
	PI-7	Information regarding botnet mitigation is always up to date	o	o	
	PI-8	There is process for customer support		o	
	PI-9	There is service level agreements (SLA)		o	
	PI-10	Security standards is adhered to		o	
DETECTION					
Customer	DC-1	Self-identity portal is presented			o
	DC-2	ISPs receive information on possible botnet attacks			o
Other	DO-3	Detected (botnet) infections is broadcasted			o
	DO-4	External parties provide information on possible infection			o
	DO-5	Information on possible attack are received from AbuseHub			
ISP	DI-6	Honeynet is applied	o		
	DI-7	Intrusion detection system (IDS) is applied	o		o
	DI-8	Infections are actively validated	o		
	DI-9	Abuse team is put in place			o
NOTIFICATION					
Customer	NC-1	Infected customers are notified		o	
	NC-2	Notifications are provided with remediation tools	o	o	
Other	NO-3	Other providers are notified about infections		o	
REMEDIATION					
Customer	RC-1	Infected customers are isolated	o	o	
	RC-2	Information to mitigate potential botnet attacks is publicised	o	o	
	RC-3	Links for professional supports are provided in case of infection		o	
Customer/Other	RV-4	information on walled garden procedure is shared		o	
Other	RO-5	Best practices for removal of infections is shared		o	
RECOVERY					
Customer	Re-1	Customer's internet connection is activated	o	o	
	Re-2	Customers are supported on recovery process		o	
	Re-3	Customers are informed of the potential impacts of recovery on personal data and accounts		o	

5.2. Prevention

Prevention is the first and most important security measure against potential cyber-attacks. Anticipatory measures such as anti-virus, anti-worms and secured routers are good endpoint security solutions (PC-1) that have proven effective against botnet infections when provided by the ISPs. Similarly, ISPs usually come up with series of security awareness programmes (training, conferences, etc.) to raise their customers' awareness on botnet threats and mitigation (PC-2). Countries have associations (national and international) of ISPs and institutions (cyber security centre, etc.) where issues regarding security are discussed and initiatives to mitigate botnets are developed (PO-4). They collaborate to share information and experiences towards mitigating botnets (PO-3).

Having realized that the safety of their customers' data also lies on the platform [8, 14], ISPs embrace measures that safeguard their operations and infrastructures. They update themselves with security information (PI-7) and apply intrusion prevention system - IPS (PI-5) and other technical measures against

bonets infections (PI-6). By embracing effective customers' supports processes (PI-8) with adequate SLAs (PI-9), they adhere strictly to industrial security standards including ISO 27006:2007 and 27002:2005 (PI-10).

5.3. Detection

Even when adequate preventions are in place, security breaches may still occur leading to system being infected and added to a botnet. This is because control may not be total especially in risk management processes such as change management where process failure is possible. Detective control is therefore required to identify errors, irregularities or attacks after their occurrences [10, 29]. Botnet detection can be classified by botmasters, bots or C&C servers. The detection could be active if classified by honeynets but passive if by IDS using either DNS-based, host-based, network-based or hybrid-detection [4]. However, for reasons yet to be fully investigated, ISPs prefer to focus on bots.

ISPs provide portals that allow their customers to self-identify bot-malware infection (DC-1) and in return, obtain information on possible attack from customers (DC-2). Similarly, ISPs share information on detected botnet infections with other shareholders (DC-3) and in return, receive information on possible attacks from both the AbuseHub (DO-5) and external parties (DO-4). ISPs apply IDSs (DI-7) to detect issues on their network, and honeynets (DI-6) for security issues around their internal operation and infrastructure. On detection of any infection, they validate the attack (DI-8) to avoid false positive and subsequently institute abuse team to handle the infection (DI-9).

5.4. Notification

An infected customer should be notified by ISPs (NC-1) once an infection is detected. Other ISPs should be adequately informed (NC-3) as well to increase awareness and avoid reoccurrence. Notification may be through email, phone calls or text/browser messages and should come with remedial measures (NC-2).

5.5. Remediation

Upon detection of infections and notifying the stakeholders (customers and other peer ISPs), ISPs take immediate remediation measures to address the compromised systems of a botnet. In which case, infected customers are isolated (RC-1) and Information to mitigate potential botnet attacks is publicised (RC-2) while links for professional supports are given to the customer (RC-3). Best practices for removal of infections is shared only to the stakeholders (RO-5) but information on processes to deal with the isolated compromised system is shared to both the customers and other stakeholders (RV-4).

5.6. Recovery

This is the final step of the mitigation measures and it is more of an extension of remediation stage. Once the infection is removed, ISPs reactivate customers' internet connection (Re-1) and provide effective customer supports throughout the recovery process (Re-2). Before recovery process commences, ISPs do ensure that customers are adequately informed of the possible impacts on their accounts and personal details (Re-3).

6. RESULTS AND DISCUSSION

This section validates the reference model used in this empirical study and interpreted the results discussed. The interviewees examined every part of the reference model for completeness and correctness to ascertain the validity and reliability of the research instrument. Common follow-up actions of mitigating botnets include: shutting down C&C-servers, hijacking C&C-servers to hack back or infiltration to dismantle the botnet from within, remote disinfection of compromised systems, unsolicited termination of customer's contracts after multiple attacks, and blocking of botmalware infected websites. This study recognises the importance of these additional actions. However, it does not extend the model to them since both the cyber security center (NCSC) and all the ISPs already affirmed that they hardly cover such actions.

This study also noticed that it is not every aspects of our model that are applicable to every ISP. This is depicted on Table 1 and summarised on Table 2 where colour Red represents aspects that are hardly applied by ISPs, Tan are adopted by just few ISPs, and Orange colour are those applied by all the ISPs in Nigeria. Although there are five security aspects that are generally not being attended to by the ISPs and nine others are being patronised by only a few, 16 out of 30 (representing 53.33%) security aspects are duly practiced by all Nigerian ISPs.

Despite that they are not the major causes of attacks [27, 30] and botnet is even expensive to mitigate, ISPs still take safety against botnet attacks very seriously. Even though, nine security aspects are not covered by two of the ISPs for administrative reasons as shown in Table 2, other 16 of 30 are covered by

all the seven ISPs leaving only five aspects representing 16.7% not being covered. We notice further on Table 1 that these 16 aspects are in ratio 7:5:4 respectively representing customers, ISPs, and others. Hence, ISPs give higher priorities to their customers' safety and are capable of performing advanced detection and follow-up actions.

Table 2. Nine security aspects

Descriptions	Aspects List	No of Aspects	No of ISPs
Aspects which ISPs hardly handle	PI5, DC1, DC2, DI6, DI7	5	
Aspects performed by just few ISPs	PI6, PI9, DO3, NO3, RC3, RV4, RO5, Re2, Re3	9	5
Aspects applied by all the ISPs	PC1, PC2, PC3, PC4, PI7, PI8, PI10, DO4, DO5, DI8, DI9, NC1, NC2, RC1, RC2, Re1	16	7

Only one out of seven interviewed ISPs implement IPS (PI5) and another one receives information on potential botnet attacks (DC2). While none of the ISPs have a portal for customers to self-identify potential botnet infection (DC1), only two apply honeynet (DI6) and another two apply IDS (DI7) in their networks even though, on a very small scale. The ISPs are generally not performing Deep Packet Inspection as they fail to monitor the contents of the traffic generated by their customers. They all attribute this failure to possible high running cost and are therefore looking at commercialising the service.

Some notable numbers of ISPs apply technical measures such as password dualisation against botnet infections (PI6). Some offer SLAs to their customers (PI9) to bind their business relationship while others broadcast botnet infection when detected (DO3) and even notify other ISPs to raise security awareness (NO3). Despite that a good number of ISPs provide links for professional supports in case of infection (RC3), information sharing on walled garden procedure (RV4) as well as sharing of best practices for removal of infections (RO5) is limited. It is only some ISPs that apply remedial measures such as customer's supports (Re2) and awareness/enlightenment (Re3) on the potential impacts of recovery on personal data and accounts. Since prevention of attacks is always better than cure [30, 31], ISPs are directing greater efforts on botnet prevention and notification. Even though they are not under any obligation to take such actions, they implement customer support processes for adequate prevention and detection [31] but little for remediation and recovery.

7. CONCLUSION

Fraudulent mails emanating from Nigeria have dented the image of Nigerian internet users. This is calling for further effective botnet mitigations as a significant number of systems are continuously being attacked. Criminals are increasingly launching sophisticated attacks on internet devices by deploying coordinated attacks such as malware threats, insider threats, data breaches (resulting from poor access controls) and system misconfigurations. Standard methods of reporting spam events, characterizing particular spam, and of sending spam control data may be helpful to fight cybercrime in Nigeria but a collaborative effort is much more required using tools and standards that boost information exchange and coordination performance.

ACKNOWLEDGEMENTS

This study was jointly sponsored by both Covenant University, Ota and First Technical University, Ibadan, Nigeria.

REFERENCES

[1] A. Longe, O.B., Chiemeke, S.C., Fashola, S., Longe, F., and Omilabu, "Internet Service Providers and Cybercrime in Nigeria Balancing Services and ICT Development," *Social Science International Journal,* vol. 6, pp. 1–11, 2007.
[2] Federal Communications Commission, "U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)," March 2012. [Online]. Available: https://itlaw.wikia.org/wiki/U.S._Anti-Bot_Code_of_Conduct_(ABCs)_for_Internet_Service_Providers_(ISPs).
[3] A. K. Sood and R. Bansal, "Prosecting the Citadel Botnet - Revealing the Dominance of the Zeus Descendent," *Virus Bulletin,* pp. 1–17, Sep. 2014.
[4] J. Pijpker and H. Vranken, "The Role of Internet Service Providers in Botnet Mitigation*," 2016 European Intelligence and Security Informatics Conference (EISIC),* Uppsala, pp. 24-31, 2016.

[5] T. Schless and H. V. Open, "Counter botnet activities in the Netherlands: a Study on Organisation and Effectiveness," *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pp. 75–82, 2013.
[6] S. H. Usman, "A review of responsibilities of internet service providers toward their customers' network security," *Journal of Theoretical and Applied Information Technology*, vol. 49, no. 1, pp. 70–78, Mar. 2013.
[7] AhelioTech "Botnets : Dawn of the connected dead," *AhelioTech*, 2017. [Online]. Available: https://www.aheliotech.com/blog/botnets-dawn-of-the-connected-dead/
[8] Q. Lone, G. C. M. Moura, and M. Van Eeten, "Towards incentivizing ISPs to mitigate botnets," *AIMS 2014: Monitoring and Securing Virtualized Networks and Services*, vol. 8508, pp. 57–62, 2014.
[9] B. Rowe, W. Dallas, R. Douglas, and B. Fern, "The Role of Internet Service Providers in Cyber Security," *Institute for Homeland Securiry Solutions*, pp. 1–10, Apr. 2009.
[10] K. O. Okokpujie, E. Noma-Osaghae, O. J. Okesola, S. N. John, and O. Robert, "Design and Implementation of a Student Attendance System Using Iris Biometric Recognition," *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, pp. 563-567, 2017.
[11] M. Integrated, "Final Report for: Development of Best Practices in Information Infrastructure Security Management," *Department Of New Media And Information Security Plot 423 Aguiyi Ironsi Way Maitama, Abuja*, pp. 1–134, 2016.
[12] N. Hachem, Y. Ben Mustapha, G.G. Granadillo, and H. Debar, "Botnets: Lifecycle and taxonomy," *2011 Conference on Network and Information Systems Security*, La Rochelle, pp. 1-8, 2011.
[13] M. van Eeten, Q. Lone, G. Moura, H. Asghari, and M. Korczyński, "Evaluating the Impact of Abuse HUB on Botnet Mitigation," *arXiv*, Dec. 2016.
[14] I. Stamatoudi, "The role of Internet Service Providers in copyright infringements," *Research Handbook on Cross-border Enforcement of Intellectual Property*, pp. 789–818, 2014.
[15] Z. Lerner, "Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets," *Harvard Journal of Law and Technology*, vol. 28, no. 1, pp. 237-261, 2014.
[16] D. R. Michel van Eetena, Johannes M. Bauer, Hadi Asghari, Shirin Tabatabaie, "The Role of Internet Service Providers in Botnet Mitigation," *Chair Innov. Regul. Digit. Serv.*, pp. 1–31, 2010.
[17] M. Van Eeten, J. M. Bauer, H. Asghari, S. Tabatabaie, and D. Rand, "The Role of ISPs in Botnet Mitigation: an Empirical Analysis Based on Spam Data," Delft Univ. Technol., 2009. [Online]. Available: https://ssrn.com/abstract=1989198
[18] H. Asghari, M. J. G. Van Eeten, and J. M. Bauer, "Economics of Fighting Botnets: Lessons from a Decade of Mitigation," in *IEEE Security & Privacy*, vol. 13, no. 5, pp. 16-23, Sep.-Oct. 2015..
[19] H. Tiirmaa-klaar, J. Gassen, and E. Gerhards-padilla, "Botnets - SpringerBriefs in Cybersecurity," *Springer*, 2019.
[20] OTA, "Botnet Remediation Overview & Practices," *Online Trust Alliance*, pp. 1–18, Oct. 2013.
[21] J. Livingood, N. Mody, and M. O'Reirdan, "Recommendations for the Remediation of Bots in ISP Networks," *Internet Engineering Task Force (IETF)*, pp. 1–29, Mar. 2012.
[22] H. Lords, "Personal Internet Security," *House Lord, Sci. Technol. Committee*, 5th Rep. Sess. 2006-07, vol. 2, pp. 1–444, 2007.
[23] Serianu, "Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness," 2016 Kenya Cyber Secur. Rep., pp. 51, 2016.
[24] Kennedy Okokpujie, Etinosa Noma-Osaghae, Olatunji Okesola, Osemwegie Omoruyi, Chinonso Okereke, Samuel John, and Imhade P. Okokpujie, "Integration of Iris Biometrics in Automated Teller Machines for Enhanced User Authentication," *International Conference on Information Science and Applications (ICISA)*, vol. 514, pp. 219–228, July 2018.
[25] E. Noma-osaghae, R. Okonigene, O. Chinonso, O. J. Okesola, and K. O. Okokpujie, "Design and Implementation of an Iris Biometric Door Access Control System," *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, pp. 590-593, 2017.
[26] O. Awodele, O. Okesola, K. Okokpujie, F. Damilola, and A. Kuyoro, "Cryptography and the Improvement of Security in Wireless Sensor Networks," in *Proceedings of the World Congress on Engineering 2018*, vol. 1, pp. 4–7, Jul. 2018.
[27] NigerianGovt, "Nigerian Telecommunication Act," *Fed. Repub. Niger. Off. Gazette, Fed. Gov. Print.*, vol. 90, no. 62, pp. 1–21, 2003.
[28] H. Asghari, "Botnet Mitigation and the Role of ISPs," Master's Thesis Delft Univ. Technol., pp. 1-187, 2010.
[29] K. Okokpujie, *et al*., "Fingerprint Biometric Authentication Based Point of Sale Terminal," *International Conference on Information Science and Applications ICISA*, vol. 514, pp. 229–238, Jul. 2018.
[30] E. N. Osaghae, K. Okokpujie, C. Ndujiuba, and O. Okesola, "Epidemic Alert System : A Web-based Grassroots Model," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 5, pp. 3809–3828, Oct. 2018.
[31] I. P. L. Png and C. Wang, "The Deterrent Effect of Enforcement against Computer Hackers: Cross-Country Evidence," *Department of Information Systems, National University of Singapore*, 2007.